https://dx.doi.org/10.22161/ijaers/4.1.1 *ISSN: 2349-6495(P) | 2456-1908(O)*

Secure Authentication Using Click Draw Based Graphical Password Scheme

Pratibha Rane, Nilam Shaikh, Prarthana Modak

Computer Engineering Department, S.S.P.M.'s College of Engineering, Kankavli, Mumbai University, India

***Abstract*—** *Graphical passwords are an alternative to alphanumeric passwords in which users click on images to authenticate themselves rather than type alphanumeric strings. We have developed one such system, called Secure Authentication using Click Draw Based graphical password scheme, and evaluated it with human users. Secure Authentication using Click Draw Based graphical password scheme, including usability and security evaluations, and implementation considerations. An important usability goal for knowledge-based authentication systems is to support users in selecting passwords of higher security, in the sense of being from an expanded effective security pace. We use the sequence of multiple images along with a dummy image and alsoa pattern on any single image to influence user choice in click draw based graphical passwords, encouraging users to select more random, and hence more difficult to guess patterns.*

Keywords—Click Draw, Cued Click Point, Graphical password, HOTSPOTS, Textual password.

I. INTRODUCTION

Authentication in the computer world refers to the act of confirming the authenticity of the user's digital identity claim. Currently, popular authentication mechanisms are mainly based the following factors: something that the user has (an object), knows (a secret), or uniquely represents him (biometric identifiers). In the simplest form, a system that requires authentication challenges the user for a secret, typically a pair of username and password. The entry of the correct pair grants access on the systems services or resources. Unfortunately, this approach is susceptible to several vulnerabilities and draw-backs. These shortcomings range from user selected weak or easily guessable passwords to more sophisticated threats such as malware and keyboard sniffers. An adversary has an abundance of opportunities to compromise the text-based password authentication mechanisms. For long time the computer industry has been in a quest for better alter-natives but without popular success: most of our current systems still use the primitive text-based authentication schemes. To amend the some of the shortcomings of the textual passwords, researchers turned their attention to passwords that utilize graphical objects. Graphical authentication has been proposed as a user-friendly alternative to password generation and authentication [3].

The main difference to textual passwords is the use if a device with graphical input: the user enters the password by clicking on a set of images, specific pixels of an image, or by drawing a pattern in a pre-defined and secret order. The proposed systems claim to provide a superior space of possible password combinations compared to traditional8-character textual passwords. This property alone renders attacks including dictionary attacks and keyboard sniffers computationally hard increasing our ability to defend against Brute-force attacks. Furthermore, according to Picture Superiority Effect Theory, concepts are more likely to be recognized and remembered if they are presented as pictures rather than as words. Thus, graphical password presumably delivers a higher usability compare to text-based password.

More specifically, two-factor authentication has been with us for a quiet time. Popular examples of two-factor authentication systems are the ATM machines: to complete any transaction, the bank customer has to carry both a bank-issued card (credit or debit card) and her personal identification number (PIN).We proposes a systemthat leverages both graphical passwords and multi-factor authentication. Our approach overcomes the limitations of the traditional password (either textual or graphical) systems. To that end, we employ graphical password. We propose a system that leverages both graphical passwords and multi-factor authentication. Our approach overcomes the limitations of the traditional password (either textual or graphical) systems.

II. EXISTING SYSTEM

2.1 Pass Point Scheme

S. Wiedenbeck ET al .proposed pass-point graphical password scheme in which on a given image password consists of a sequence of 5 different click points. For password creation user selects any pixel in the image as a click-points and for login the user has to enter the same series of clicks incorrect sequence within a system defined tolerance square of original click-points. The problem with this scheme is the HOTSPOTS(the area of an image where user more likely to select the click-point)and it is easy for attackers to guess the password because user forms certain patterns in order to remember

https://dx.doi.org/10.22161/ijaers/4.1.1 *ISSN: 2349-6495(P) | 2456-1908(O)*

the secret code which results pattern formation attacks are easily possible. Thus the pass-point system suffers from these two major disadvantages. To overcome these disadvantages next technique is to be implemented.

Fig. 1: Pass Point Scheme

2.1.2 Cued Click Point

Cued Click Points was designed to reduce patterns and to reduce the usefulness of hotspots for attackers. Instead of five click-points on one image, CCP uses one click-point on five different images [2]. The next image displayed is based on the location of the previously entered click-point; it creates a path through an image set. Creating a new password with different click-points results in a different image sequence. One best feature of Cued Click Point is that the explicit indication of authentication failure is only provided after the final click-point, to protect against incremental guessing attacks. But this technique has several disadvantages like false accept (the incorrect click point can be accept by the system) and false reject (the click-point which is to be correct can be reject by the system).In this system pattern formation attack is reduced but HOTSPOT remains since users are selecting their own click-point.

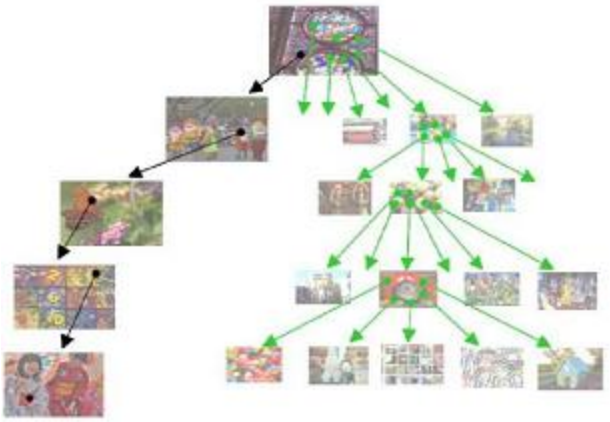

Fig. 2: Cued Click Point Scheme

2.1.3 Persuasive Cued Click Points

For creating Persuasive Cued Click Points persuasive feature is added to CCP. PCCP encourages users to select less predictable passwords. For password creation PCCP uses terms like viewport and shuffle [3]. When users creating a password, the images are slightly shaded except for a viewport as shown in the Fig 3. To avoid known hotspots the viewport is positioned randomly. The most useful advantage of PCCP is attackers have to improve their guesses. Users have to select a click-point within the highlighted viewport and cannot click outside of the viewport unless they press the shuffle button to randomly reposition the viewport.

At the time of password creation users may shuffle as often as desired but it slows the process of password creation. Only at the time of password creation, the viewport and shuffle button appears. After the password creation process images displayed normally without the viewport and shuffle button. Then user has to select correct click on particular image. PCCP is a good technology but has security problems. Fig. shows the password creation process including viewport and shuffle button [4].

Fig.3: Password Creation in PCCP, Highlighted Area is Viewport

III. LIMITATION OF EXISTING SYSTEM

Existing system have following limitations:

1) Random placement of the viewport makes it difficult to remember the click points.

2) User may use the shuffle for selecting the noticeable hotspots that can be guessable and hence prone to attacks.

3) Thus there is again a choice between remembrance and security

IV. PROPOSED SCHEME

The purpose of click-draw based graphical password scheme (CD-GPS) is to enhance the image-based authentication in both security and usability. There are mainly two steps in this scheme:

1. Image selection.
2. Secret drawing.

https://dx.doi.org/10.22161/ijaers/4.1.1 *ISSN: 2349-6495(P) | 2456-1908(O)*

4.1 Image selection

In CD-GPS, the first step is the image selection. In this step users have to select several images from an image pool. Suppose there are N1 images in the image pool, then at first users should select n N1 images from the image pool in an order and remember this order of images like a story. Users should further choose k n image from the above selected n images. k is nothing but the single image on which we have to draw secret.

Fig. 4: Image Selection

4.2 Secret drawing

This is the second step comes after the image selection. In this step users can freely click-draw their secrets. For constructing secret drawing users use series of clicks as shown in above fig. the image is divided into a 1616table. Users can use the coordinate numbers for remembering their drawings. In above fig. user draw number 7 as the secret, which consists of coordinates (1, 5), (1, 6), (1, 7), (2, 7), (3, 7), (4, 7) and (5, 7). In this technique there is not necessity to remember the sequence of clicks. During the authentication, users should re-draw their secrets accurately in the correct coordinates on the image.

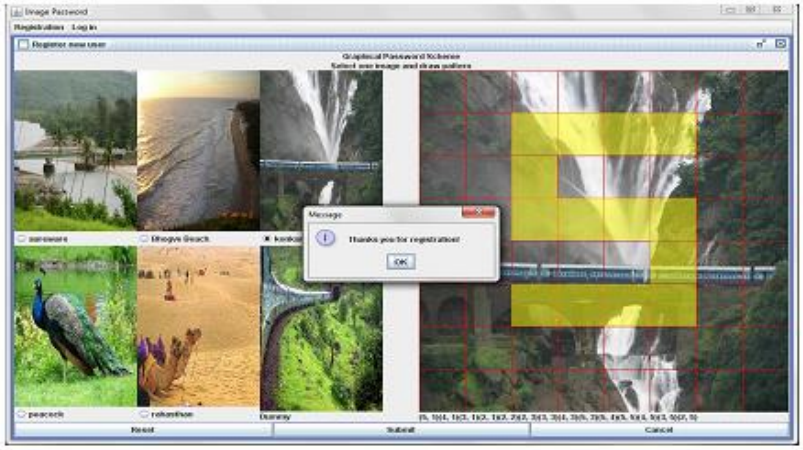

Fig. 5: Secret Drawing

V. CONCLUSION AND FUTURE WORK

A knowledge based authentication system that uses set of ordered images with pattern drawn on it. It satisfies both conflicting requirements i.e. it is easy to remember and it is hard to guess. By implementing more complex configurations like more number of images with some dummy images, one can achieve more security .It is more difficult to break graphical passwords using the traditional attack methods such as brute force search, dictionary attack or spyware.

In future, we can give the facility of "Change password" for the users through which any user of this system can change the password when he/she want. Also, we can use this secure system for Web based Application. We can create Administrator who handles all the privileges, such as Reset the password, insert new images into the database etc.

REFERENCES

[1] "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-

https://dx.doi.org/10.22161/ijaers/4.1.1 *ISSN: 2349-6495(P) | 2456-1908(O)*

Based Authentication Mechanism" , *Sonia Chiasson, Member, IEEE, Elizabeth Stobert, Student Member, IEEE, Alain Forget, Robert Biddle, Member, IEEE, and Paul C. van Oorschot, Member, IEEE*

[2] "Graphical Password Authentication Using Cued Click Points" *,Sonia Chi-asson1,2, P.C. van Oorschot1, and Robert Biddle2, version: June 29, 2007 ESORICS2007, Dresden Germany, September 2007. J. Biskup and J. Lopez (Eds.): ESORICS 2007,LNCS 4734, pp.359-374, 2007. c Springer-Verlag Berlin Heidelberg 2007*

[3] "Graphical Passwords: A Survey",*Xiaoyuan Suo Ying Zhu G. Scott. Owen Department of Computer Science, Georgia State University Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC 2005) 1063-9527/05 20.00 2005IEEE*

[4] A Book, "Persuasive Technology: Using Computers to Change What We Think and Do", *by, B. J. Fogg.*